UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

FILED
NOV 14 2007
CLERK, U.S. DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
BY DEPUTY

In the Matter of the Search of

Hewlett Packard Touch Smart 1Q770 computer
Serial Number: CNH7010011

APPLICATION AND AFFIDAVIT

FOR SEARCH WARRANT

CASE NUMBER: '07 MJ 2656

I, Jodi A. Jewett, being duly sworn depose and say:

I am a Special Agent with the Federal Bureau of Investigation, and have reason to believe that property or premises known as:

See Attachment A

in the Southern District of California there is now concealed a certain person or property, namely,

See Attachment B

which is: Subject to seizure under Rule 41(b)(1) of the Federal Rules of Criminal Procedure because the property constitutes evidence of the commission of criminal offenses or instrumentalities used in committing criminal offenses. The criminal offenses at issue are violations of: (1) Title 18, United States Code, Section 2251, production of child pornography as it relates to interstate or foreign commerce; (2) Title 18, United States Code, Section 2252A(a)(5)(B), possession of child pornography; (3) Title 18 United States Code Section 2252A(a)(2)(A), distribution receipt or distribution of child pornography, and Title 18, United States Code, Section 2252A(a)(2)(B), receipt or distribution of material containing child pornography.

The facts support a finding of Probable Cause are as follows:

See Affidavit of Jodi A. Jewett

Continued on the attached sheet and made a part thereof. X Yes __ No

Jodi A. Jewett
Special Agent
Federal Bureau of Investigation

Sworn to before me, and subscribed in my presence

11/9/07 at San Diego, California
Date City and State

CATHY ANN BENCIVENGO
UNITED STATES MAGISTRATE JUDGE
Name and Title of Judicial Officer

Signature of Judicial Officer

AFFIDAVIT OF JODI JEWETT
IN SUPPORT OF SEARCH WARRANT

I, Jodi A. Jewett, being duly sworn, do hereby depose and say:

BACKGROUND AND EXPERIENCE OF AFFIANT

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") assigned to the Riverside resident agency in Riverside, California, and have been so employed since September 2006. I am assigned to a multi-agency child exploitation task force known as the Southern California Regional Sexual Assault Felony Enforcement Team ("SAFE Team"). As a SAFE Team member and an FBI agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography. I am responsible for enforcing federal criminal statutes involving the sexual exploitation of children, and have conducted numerous investigations involving the possession, importation, and distribution of child pornography. I have completed approximately 136 hours of training in crimes against children, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also participated in the execution of numerous search warrants, many of which involved child exploitation and/or child pornography.

//

//

//

PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of a search warrant for four computers[1] seized during the execution of a search warrant on July 24, 2007, for evidence of violations of Title 18, United States Code, Section 2251, production of child pornography as it relates to interstate or foreign commerce, Title 18, United States Code, Section 2252A(a)(5)(B), possession of child pornography, Title 18 United States Code, Section 2252A(a)(2)(A), distribution receipt or distribution of child pornography, and Title 18 United States Code, Section 2252A(a)(2)(B), receipt or distribution of material containing child pornography.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. This affidavit is intended to show that there is sufficient probable cause for the requested search warrant and does not purport to set forth all of my knowledge of or investigation into this matter.

THE ITEMS TO BE SEARCHED

4. The items to be searched consist of four computers recovered by the California Department of Justice ("CAL-DOJ") on July 24, 2007, from the residence of JAMES ALBERT SWEENEY II ("SWEENEY") located at 4555 Mission Inn Avenue, Riverside, California 92501. SWEENEY is currently under investigation for a fraudulent scheme by CAL-DOJ.

---

[1] The term "computer" as used in this affidavit, is defined by 18 U.S.C. § 1030(e)(1).

5. The computers consist of the following:

a. Hewlett Packard M7000 desktop computer, bearing serial number MXK60804L3;

b. Dell Dimension E521 desktop computer, bearing serial number HWC16C1;

c. Hewlett Packard Touch Smart 1Q770 computer, bearing serial number CNH7010011; and

d. Sony Vaio laptop computer, bearing serial number VGNUX280P.

6. The four computers, as described above, are currently in the custody of the Regional Computer Forensics Laboratory ("RCFL") in San Diego, California. Additional computers were also seized by CAL-DOJ investigators from SWEENEY's business and storage facility, however, those computers are not a subject of this search warrant.

THE ITEMS TO BE SEIZED

7. Based on the facts set forth in this affidavit, and my experience investigating computer crimes as relates to crimes against children, I submit that there is probable cause to believe that the computers described above will contain evidence of violations of: Title 18, United States Code, § 2251, production of child pornography as it relates to interstate or foreign commerce, Title 18, United States Code, § 2252A(a)(5)(B), possession of child pornography, Title 18 United States Code, § 2252A(a)(2)(A), receipt or distribution of child pornography, and Title 18 United States Code, § 2252A(a)(2)(B), receipt or distribution of material containing child pornography.

8. More specifically, as described below, I believe that there is probable cause that evidence of the following will be found on the four computers as listed in ATTACHMENT A:

a. Files or records that tend to identify the person(s) in control, possession, and ownership of the computers identified in ATTACHMENT A or of any other computers, including, but not limited to, canceled mail, photographs, personal telephone books, diaries, bills and statements, identification cards and documents, airline tickets and related travel documents, bank books, checks, and check registers, public storage facilities receipts, computer registration records and sales receipts;

b. Images of child pornography, or materials containing child pornography as defined in 18 U.S.C. Section 2256, which visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography;

c. Files and records reflecting ownership, purchase, possession, or use of computer devices or peripherals such as web cameras and other video and audio recording devices, that could be used to transmit live images over the Internet or record images for later transmission over the Internet;

d. Files and records relating to the provision of internet service, including billing and toll records;

e. Correspondence that are indicia of production, possession, receipt, or distribution of child pornography including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, receipt, production, distribution, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

f. Correspondence relating or referring to exploitation of children including, but not limited to electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce of child pornography as defined in 18 U.S.C. § 2256, including by United States mail or by computer.

g. Files and records pertaining to possession, production, receipt or distribution of child pornography, as defined in 18 U.S.C. § 2256, including but not limited to:

(1) Envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

(2) Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or

foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

h. Any files or records relating to the exploitation of minors.

i. Any files or records identifying individual e-mail addresses and internet chat room names;

j. Any files or records showing the acquisition and/or sale of computer hardware, computer software, computer documentation, and/or computer passwords and other data security devices;

k. Any files or records evidencing occupancy or ownership of any residences and storage units registered to, owned by, or controlled by JAMES ALBERT SWEENEY II, including, but not limited to copies of utility and telephone bills, mail envelopes, addressed correspondence canceled mail, photographs, personal telephone books, diaries, bills and statements, identification cards and documents, airline tickets and related travel documents, bank books, checks, and check registers, and public storage facilities receipts.

l. Any files, records, programs, application or materials, including but not limited to, images and electronically stored computer data that would lead to the identity of any minors as depicted in electronic images or evidenced in electronic communications.

m. Mailing lists, mailing address labels and any and all documents and records pertaining to any correspondence between JAMES ALBERT SWEENEY II and any minor.

n. Any files or records related to ownership, control and use of digital cameras, camcorders, or other recording devices.

o. Electronic materials pertaining to the receipt of, or orders or requests for visual depictions of a minor involved in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

p. Names, lists of names or addresses and identifying information of minors (such as names and dates of birth of minors).

q. As used above, the terms files, records, programs, or correspondence includes files, records, programs, or correspondence created, modified or stored in any form including electronically.

TIMING OF SEARCH

9. As noted, the computers are currently in the possession of RCFL. The computers will be searched by RCFL at the San Diego facility upon authorization of this warrant. Consistent with the requirements of Rule 41, the computers will be delivered to a computer forensic technician at RCFL within 10 days of the effective date of this warrant to commence the search. For the reasons noted in paragraph 22 below, the search will not be completed during the 10-day period. However, the computers will be imaged, and will be preliminarily examined to determine whether they contain any evidence or are an instrumentality of a

crime, within 60 days. If the computer forensic technicians determine that the data does not fall within any of the items to be seized pursuant to this warrant or is not otherwise legally seized, the government will return these items within a reasonable period of time not to exceed 60 days from the date of execution of the warrant. If the government needs additional time to determine whether the data falls within any of the items to be seized pursuant to this warrant, it must obtain an extension of the time period from the Court within the original sixty day period.

INVESTIGATION

10. On or about October 2, 2007, I was contacted by Riverside Police Department ("RPD") Detective James Dana and CAL-DOJ Investigator Aaron L. Ward (Investigator Ward), who provided me with the following information:

a. On July 24, 2007, CAL-DOJ executed a state search warrant for evidence of fraud and grand theft, to include any computer systems found, at SWEENEY's residence, storage facility and business. Pursuant to the state fraud investigation and execution of the state search warrants attached hereto as ATTACHMENTS C and D, several of SWEENEY's computer systems were seized. The items to be searched, as described in ATTACHMENT A, were seized from SWEENEY's residence.

b. Investigator Ward was a member of the law enforcement team that searched SWEENEY's residence on July 24, 2007.

c. Prior to conducting the search, Investigator Ward confirmed that SWEENEY owned the residence located at 4555 Mission Inn Avenue, Riverside California and that SWEENEY was receiving mail at that residence. I further confirmed with the United States Post Office, during the week of October 8, 2007, that SWEENEY was the only person receiving mail at that residence.

d. During the search of SWEENEY's residence, Investigator Ward observed and later informed me of the following:

(1) SWEENEY had two dogs on the premises, tan colored dog that appeared to be a Golden Retriever and a small dog that appeared to be a Chihuahua.

(2) The furniture in SWEENEY's residence was ornate and rich looking.

(3) The bed in SWEENEY's master bedroom appeared to be queen sized. The bed was framed in heavy, dark wood.

(4) A Hewlett Packard M7000 desktop computer was seized from SWEENEY's home office, upstairs across the hallway from his master bedroom.

(5) Other computer systems, as described above, were seized from SWEENEY's residence and storage facility.

e. The Hewlett Packard M7000 desktop computer, along with the other computers seized pursuant to the execution of the search warrant were sent to RCFL in San Diego, California for analysis by Investigator Ward.

f. On September 14, 2007, Investigator Ward spoke with Riverside County Sheriff's Office Detective Peter Felt. ("Detective Felt"). Detective Felt is a member of the Riverside Computer and Technology Crime High-Technology Response Team (C.A.T.C.H.). Detective Felt is currently assigned to the RCFL in San Diego, California and was responsible for imaging and analyzing the computers submitted by Investigator Ward. Detective Felt told Investigator Ward that in analyzing the Hewlett Packard M7000 desktop computer seized from SWEENEY's home office, Detective Felt discovered what appeared to be evidence of child pornography.

11. Based upon my review of that state search warrants executed by CAL-DOJ (see ATTACHMENTS C and D) I have learned the following:

a. In his original affidavit, Investigator Ward requested that "investigating officers, and those agents acting under the direction of the investigating officer, be authorized to access all computer data to determine if the data contains property, records, and information . . . ." (See page 17 of ATTACHMENT C). Investigator Ward further explained that "the file name in the folder/directory is not a reliable indicator of the true nature of its contents, especially where there may be a desire on the user's part to conceal certain records" (see page 14 of ATTACHMENT C). Investigator Ward also provided that "computer users may also conceal data through a number of methods, including the use of misleading filenames and extensions. For example, files with the extension .jpg are digital image files. However, a computer user could change a .jpg file extension to .txt or .dll, in order to create an appearance that a digital image is actually a text or system file." (See page 14 of ATTACHMENT C)

b. Investigator Ward incorporated the original affidavit, (ATTACHMENT C), into the supplemental affidavit, (ATTACHMENT D), as indicated on page 2 of ATTACHMENT D. Investigator Ward referred to the original affidavit as exhibit 1. (See page 2 of ATTACHMENT D). Exhibit 1 refers to the original affidavit and is now attached to this document as ATTACHMENT C. Investigator Ward indicated that "Records in the form of electronic files stored on computers will be treated as indicated in Exhibit 1, pages 12-17." (See page 6 of ATTACHMENT D).

c. Accordingly, after issuance of the search warrants, Detective Felt conducted an initial preview of the computer. While conducting this initial preview, Detective Felt came upon an image, in plain view, that appeared to be child pornography.

12. On November 8, 2007, Detective Felt advised me about the specifics of conducting the computer analysis. Detective Felt told me that to analyze the computer for evidence and instrumentalities of the crimes alleged in the state search warrant, Detective Felt did the following:

a. Detective Felt first made an image of the hard drive of the Hewlett Packard M7000. Detective Felt then used the Forensics Took Kit ("FTK") software in order to put the data copied from the hard drive into separate containers. Containers are the method of organization used by FTK to separate computer data into workable sections. Containers are assigned according to the information that is put into them, and such containers include: graphics, documents, email, explorer, search, and overview containers. An item can be placed into more than one container, based upon content. For example, a word document that contains an image such as a business logo on it's letterhead, would be placed into both the document and image containers. Additionally a document could have been scanned and saved into the computer, which would place it in the graphics container, though it was originally a document. Therefore, the names given to such containers can be misleading and it should not be assumed that a document that contains evidence of a crime could not reasonably be found in an image container.

b. In conducting his initial preview and beginning the forensic analysis of the Hewlett Packard M7000 imaged hard drive, Detective Felt previewed each container that the FTK software had generated. This is done both to ensure that the FTK software functioned correctly and to attain an initial look at potential evidence. Since any type of document could reasonably be placed in any of the FTK containers, depending upon how it was saved; all containers are examined in a standard forensic analysis. When Detective Felt looked in the graphics container for documents and records pertaining to the fraud investigation, he came upon an image, in plain view, that appeared to be child pornography.

13. Investigator Ward further advised me on October 2, 2007 of the following:

a. On September 14, 2007, Detective Felt further told Investigator Ward that Detective Felt discovered what appeared to be one digital pornographic image and various other digital images of young boys not fully dressed during his analysis.

b. The pornographic image showed a picture of a young boy, who appeared to be approximately twelve to fourteen years of age. In this photograph, the boy is standing near one side of a bed in what appears to be a bedroom at a residence. The bed depicted in this image is framed in heavy, dark wood. The young boy is wearing jeans and a blue t-shirt. Two dogs, one dark colored and the other tan in color, are also seen lying on the bed. The boy in the picture is holding his erect penis in one hand while the dark colored dog appears to be licking the boy's penis.

c. In a second digital photograph, an adult male is seated on the opposite side of the same bed where the boy was standing in the pornographic image described above in paragraph 10(f)(3). The adult male is wearing a t-shirt and underwear and is holding a laptop computer in his lap. Investigator Ward further described the laptop as a Sony Vaio. The two dogs from the pornographic image are also seen in this picture.

d. In both pictures described in paragraphs 10(f)(3) and 10(f)(4) above, the dogs appear to be lying in the same place. In the picture featuring the adult male, the dogs are on the left side of the bed near the adult male's feet. In the pornographic picture, the dogs are on the left side of the bed in the same position as in the picture featuring the adult male. Detective Felt also noted that the bed, the bedspread, and the lighting appeared to be the same in both pictures. Detective Felt stated that the camera angle changed between the two photographs and the different angles would have allowed for both the adult male and the twelve to fourteen year old boy to be in the same location at the same time and be featured in two different photographs.

e. Based on his training and experience, Detective Felt believed that these two photographs were taken at approximately the same time and at the same location.

14. On September 18, 2007 Investigator Ward met with Detective Felt at the RCFL in San Diego, California. The images described above were shown to Investigator Ward. After this meeting, Investigator Ward told me that he recognized the bed in the two photographs as being the bed that Investigator Ward saw at SWEENEY's residence during the execution of the search warrant at 4555 Mission Inn Avenue in Riverside California on July 24, 2007.[2] Investigator Ward looked at the second photograph

---

[2] Although investigators did not see the dark colored dog depicted in the pornographic image when at SWEENEY's residence during execution of the search warrant on July 24, 2007, it is unclear wether the tan colored dog was one of the two dogs seen at SWEENEY's residence during execution of the search warrant.

involving the adult male as described in paragraph 10(f)(4) above and told me that he recognized the adult male seated on the bed as SWEENEY.[3] Investigator Ward made the identification of SWEENEY based on looking at photographs of SWEENEY and from personally meeting SWEENEY on August 21, 2007.

15. I subsequently learned that SWEENEY was the registered owner of the residence located at 4555 Mission Inn Avenue Riverside CA 92501 by conducting a query of the ACCURINT database. The query revealed that the residence was registered to James A. SWEENEY II. I then confirmed SWEENEY's name as it appears on his California driver's license, number DXXXX259, as James Albert Sweeney II.

16. I also learned that SWEENEY owns a second residence in Afton, Tennessee. A query of the ACCUPRINT database for this residence in Tennessee also revealed that James A. Sweeney II was the registered owner of that residence.

17. On October 3, 2007, I learned that at some time after execution of the CAL-DOJ search warrant on July 24, 2007, SWEENEY's attorney advised CAL-DOJ investigators that SWEENEY was currently staying at the residence in Tennessee.

18. I also learned thereafter that Detective Felt relayed the following information to Investigator Ward:

---

[3] The computer depicted in the photo of SWEENEY seated on the bed has not been seized by law enforcement authorities and its location is currently unknown. The Sony Vaio currently in the possession of RCFL is a small sized Sony Vaio where as the Sony Vaio laptop depicted in the image as described in paragraph 10(f)(4) above is a full size laptop.

a. During his initial preview of the Hewlett Packard M7000 desktop computer, Detective Felt also viewed a number of other images of young boys in various stages of undress.

b. One of these images was a photograph of a young boy, approximately ten years old, in a bathtub. The boy seated in the bathtub can only be seen from the waist up.

c. Similarly, in many of the other photographs, the boys were shirtless with their pants pulled low, but not exposing their pubic area.

d. Detective Felt also retrieved five images from the Hewlett Packard M7000 desktop computer for purposes of identifying the individuals depicted in these images. Detective Felt chose the five images to include the faces of four boys he had seen most frequently during his preview of the Hewlett Packard M7000 computer, including the face of the boy seen in the child pornography image described in paragraph 10(f)(3) above.

e. Within these five preliminary images, Detective Felt included one image that included the adult male seen on the bed as described in paragraph 10(f)(4) above. These preliminary images, hereinafter referred to as "Preliminary Images" 1, 2, 3, 4, and 5 are further described below:

(1) Preliminary Image 1 depicts a teenaged boy with dirty blond hair, brown or hazel eyes, and a grimace on his face. The boy is wearing a grey t-shirt and a white beaded necklace with three red beads spaced within the white beads of the necklace. The individual depicted in Preliminary Image 1 is the same individual

depicted in the child pornography image as described in paragraph 10(f)(3) above.

(2) Preliminary Image 2 depicts a young boy with shaggy blond hair and brown or hazel eyes. The boy is wearing blue jeans and a grey t-shirt with the word "etnies" in white letters on the front of the t-shirt. The boy is standing with his right hand behind his head and his left hand pulled to the left underarm. The boy is wearing what appears to be black wrist braces on both wrists.

(3) Preliminary Image 3 depicts a young boy with short, dirty blond hair and brown or hazel eyes. The boy is wearing a black t-shirt with a red thorn-like line across the chest. The boy is displaying the peace sign with his left hand.

(4) Preliminary Image 4 depicts a young boy with blond hair and blue eyes. The boy is wearing a green sweatshirt with the word "quicksilver" in white letters across the front of the sweatshirt. The boy is standing or sitting near a red leather chair and a statue can be seen behind him.

(5) Preliminary Image 5 depicts the same teenaged boy as in Preliminary Image 1. In this image, the boy is wearing a blue t-shirt and what appears to be the same white necklace. The boy is standing behind and to the left of an adult male. The adult male is SWEENEY. SWEENEY is wearing a yellow sweatshirt and a baseball cap with an unknown symbol on the front.

19. On October 2, 2007, a conference call was conducted between myself, Investigator Ward, and Detective Dana, where I learned the following:

a. Investigator Ward positively identified the location at which the pornographic photograph described in paragraph 10(f)(3) above was taken. Investigator Ward stated that when the search of SWEENEY's residence was conducted on July 24, 2007, Investigator Ward was in the residence and recalled seeing the bed in SWEENEY's bedroom as seen in both the pornographic image and the image of SWEENEY sitting on the bed.

b. Investigator Ward further advised that when he viewed the photograph depicting SWEENEY sitting on the bed, he believed that the photograph had been taken recently. Investigator Ward stated that SWEENEY, whom he identified as the adult male on the bed, looked the same in that photograph as he did when he met with SWEENEY on August 21, 2007. Investigator Ward further stated that the furniture, specifically the bed, looked to be the same as the furniture that Investigator Ward encountered during the execution of the search warrant.

20. Further investigation into this matter was conducted by myself and Detective Dana. On October 2, 2007, Detective Dana and I went to SWEENEY's residence located at 4555 Mission Inn Avenue, in Riverside California and observed the following:

a. From our observation through the front window of the residence, the residence appeared to be occupied and the lights including the television were on;

b. Detective Dana and I approached the front door of the residence and observed a small child sized bicycle laying on its side in the front hallway near the stairway. A stuffed animal was also seen placed on a window sill.

c. A white Chevrolet pickup truck was parked in the back driveway of the residence bearing California license plate number 7R75106. A query of this license plate returned a result for an Ernest L. Werkheiser of Milditas, California.

21. Detective Dana then obtained RPD Report P07-072881 regarding a police contact on May 13, 2007 at SWEENEY's residence located at 4555 Mission Inn Avenue, Riverside, California. The report provided the following:

a. RPD Officer J. Mattson responded to a drunk in public call located at the residence. Upon arrival, SWEENEY told Officer Mattson that he was a family friend of the Williams family. SWEENEY told the officer that Kenneth Dale Williams ("Mr. Williams") is a homeless father with four sons, and Mr. Williams drops off his sons at SWEENEY's residence every morning for purposes of preparing for school.

b. On May 13, 2007, Mr. Williams left one of his sons, age fourteen, with SWEENEY. When Mr. Williams came back to SWEENEY's residence to pick up his son, SWEENEY thought that Mr. Williams was under the influence and called the RPD.

c. Mr. Williams' son told Officer Mattson that his father, Mr. Williams, beat him and his brothers. Officer

Mattson visually examined the child but was unable to locate any signs of physical abuse.

22. On October 4, 2007, Preliminary Images 1 - 5 as described in paragraphs 14(e)(1-5), were taken to the "Circle of Life" homeless shelter where Mr. Williams and his four sons had been residing for the past three years. Carrie Walker ("Ms. Walker"), is a staff member at the shelter and provided the following information:

a. Ms. Walker has known the Williams family for the past three years. Ms. Walker positively identified all the individuals depicted in Preliminary Images 1 - 5.

b. Ms. Walker identified the four young boys depicted in Preliminary Images 1 - 5 as Mr. Williams' sons.

c. Ms. Walker also identified the adult male depicted in Preliminary Image 5 as the man that the children referred to as "Uncle Jimmy." Ms. Walker further stated that the boys spoke fondly of "Uncle Jimmy" and they told Ms. Walker that Uncle Jimmy bought them expensive toys and video games.

d. Ms. Walker further stated that she last saw the Williams family approximately one month ago wherein they told Ms. Walker that they were moving in with a family in Arkansas.

e. Ms. Walker advised that Mr. Williams had stopped allowing his sons to go to "Uncle Jimmy's" residence, but never stated why. Mr. Williams told Ms. Walker that he was getting his life back together and it was time to take care of his sons.

f. Ms. Walker stated that she met "Uncle Jimmy" once, approximately three weeks prior to October 4, 2007 when "Uncle Jimmy" came to the shelter looking for the Williams family.

g. Ms. Walker provided copies of the Social Security Cards for Mr. Williams and all four of his sons. She also provided a photograph of Mr. Williams and a copy of his California Driver's License.

23. After researching various databases by using the social security numbers provided by Ms. Walker, I was able to determine that the four boys depicted in Preliminary Images 1 -5 currently range from ages ten to sixteen years old.

USE OF CAMERAS AND COMPUTERS

24. Based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I am aware of the following regarding the use of computers and cameras relating to child pornography and child exploitation:

a. The development of computers has revolutionized the way in which those who seek out child pornography are able to obtain this material. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

b. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera. The camera is attached, using a device such as a cable, or digital images are often uploaded from the camera's memory card, directly to the computer. Images can then be stored, manipulated, transferred, or printed directly from the computer. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography.

c. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) websites that offer images of child pornography. Those who seek to obtain images or videos of child pornography can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute or receive child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions involving those who wish to gain access to child pornography over the Internet. Sometimes, the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient's computer, in order to look for "footprints" of the websites and images accessed by the recipient.

d. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy or compact disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media used in home computers (commonly referred to as a hard drive) has grown tremendously within the last several years. Hard drives with the capacity of 40 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Moreover, electronic files downloaded to a hard drive can be stored for years at little to no cost.

e. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed, than on a particular user's operating system, storage capacity, and computer habits.

f. Individuals who commit crimes against children via computers do not readily discard the computer, as computers are expensive items that are typically used for years before being upgraded or discarded.

g. Individuals who commit these types of crimes often keep electronic records of activities on their computers. This information often includes logs of fraudulent transaction history, monies received, individuals that have been victimized, and payments to or from co-conspirators.

h. Individuals who possess child pornography often store evidence of child pornography on multiple computer systems and storage devices.

i. The memory cards in digital cameras have the capacity to store hundreds, if not thousands, of digital photographs.

j. Individuals who utilize digital cameras upload their digital photos from the memory cards of digital cameras to their computers, zip drives or other electronic storage devices for viewing, printing and storing.

k. Individuals who possess images of child pornography tend to trade or distribute their images on the internet for the purpose of receiving additional child pornography images.

25. Based on the foregoing, I believe additional evidence of violations of Title 18, United States Code, Section 2251, production of child pornography as it relates to interstate or foreign commerce, Title 18, United States Code, Section 2252A(a)(5)(B), possession of child pornography, Title 18 United States Code, Section 2252A(a)(2)(A), distribution receipt or distribution of child pornography, and Title 18 United States Code, Section 2252A(a)(2)(B), receipt or distribution of material containing child pornography exists on the other computer systems that were seized from SWEENEY's residence.

COMPUTER DATA

26. Based upon my training, experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing fifteen gigabytes of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 7.5 million pages of data, which, if printed out, would completely fill a 10' x 12' x 10' room to the ceiling.

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

CONCLUSION:

27. Based upon the foregoing, I believe that there is probable cause to believe that the (1) Hewlett Packard M7000 desktop computer, bearing serial number MXK60804L3, (2) a Dell Dimension E521 desktop computer, bearing serial number HWC16C1, (3) a Hewlett Packard Touch Smart 1Q770 computer, bearing serial

number CNH7010011, and (4) a Sony Vaio laptop computer, bearing serial number VGNUX280P, contain evidence of violations of Title 18, United States Code, Section 2251, production of child pornography as it relates to interstate or foreign commerce, Title 18, United States Code, Section 2252A(a)(5)(B), possession of child pornography, Title 18 United States Code, Section 2252A(a)(2)(A), distribution receipt or distribution of child pornography, and Title 18 United States Code, Section 2252A(a)(2)(B), receipt or distribution of material containing child pornography.

Jodi Jewett

Jodi A. Jewett
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
this 9th day of November, 2007

UNITED STATES MAGISTRATE JUDGE
CATHY ANN BENCIVENGO

ATTACHMENT A

ITEMS TO BE SEARCHED

The ITEMS TO BE SEARCHED are further described as follows:

a. Hewlett Packard M7000 desktop computer serial number MXK60804L3 and all hardware and software attached to, or otherwise accompanying this computer as seized;

b. Dell Dimension E521 desktop computer serial number HWC16C1 and all hardware and software attached to, or otherwise accompanying this computer as seized;

c. Hewlett Packard Touch Smart 1Q770 computer serial number CNH7010011 and all hardware and software attached to, or otherwise accompanying this computer as seized;

d. Sony Vaio laptop computer serial number VGNUX280P and all hardware and software attached to, or otherwise accompanying this computer as seized;

ATTACHMENT B

ITEMS TO BE SEIZED

1. The following are the ITEMS TO BE SEIZED from the ITEMS TO BE SEARCHED, which constitute evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 2251, production of child pornography as it relates to interstate or foreign commerce, Title 18, United States Code, Section 2252A(a)(5)(B), possession of child pornography, Title 18 United States Code, Section 2252A(a)(2)(A), distribution receipt or distribution of child pornography, and Title 18 United States Code, Section 2252A(a)(2)(B), receipt or distribution of material containing child pornography:

a. Files or records that tend to identify the person(s) in control, possession, and ownership of the computers identified in ATTACHMENT A or of any other computers, including, but not limited to, canceled mail, photographs, personal telephone books, diaries, bills and statements, identification cards and documents, airline tickets and related travel documents, bank books, checks, and check registers, public storage facilities receipts, computer registration records and sales receipts;

b. Images of child pornography, or materials containing child pornography as defined in 18 U.S.C. Section 2256, which visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography;

c. Files and records reflecting ownership, purchase, possession, or use of computer devices or peripherals such as web cameras and other video and audio recording devices, that could be used to transmit live images over the Internet or record images for later transmission over the Internet;

d. Files and records relating to the provision of internet service, including billing and toll records;

e. Correspondence that are indicia of production, possession, receipt, or distribution of child pornography including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, receipt, production, distribution, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

f. Correspondence relating or referring to exploitation of children including, but not limited to electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce of child pornography as defined in 18 U.S.C. § 2256, including by United States mail or by computer.

g. Files and records pertaining to possession, production, receipt or distribution of child pornography, as defined in 18 U.S.C. § 2256, including but not limited to:

(1) Envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat

logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

(2) Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

h. Any files or records relating to the exploitation of minors.

i. Any files or records identifying individual e-mail addresses and internet chat room names;

j. Any files or records showing the acquisition and/or sale of computer hardware, computer software, computer documentation, and/or computer passwords and other data security devices;

k. Any files or records evidencing occupancy or ownership of any residences and storage units registered to, owned by, or controlled by JAMES ALBERT SWEENEY II, including, but not limited to copies of utility and telephone bills, mail envelopes, addressed correspondence canceled mail, photographs, personal telephone books, diaries, bills and statements, identification cards and documents, airline tickets and related travel documents, bank books, checks, and check registers, and public storage facilities receipts.

l. Any files, records, programs, application or materials, including but not limited to, images and electronically stored computer data that would lead to the identity of any minors as depicted in electronic images or evidenced in electronic communications.

m. Mailing lists, mailing address labels and any and all documents and records pertaining to any correspondence between JAMES ALBERT SWEENEY II and any minor.

n. Any files or records related to ownership, control and use of digital cameras, camcorders, or other recording devices.

o. Electronic materials pertaining to the receipt of, or orders or requests for visual depictions of a minor involved in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

p. Names, lists of names or addresses and identifying information of minors (such as names and dates of birth of minors).

q. As used above, the terms files, records, programs, or correspondence includes files, records, programs, or correspondence created, modified or stored in any form including electronically.

ATTACHMENT C

ATTACHMENT D

ATTACHMENT A

ITEMS TO BE SEARCHED

The ITEMS TO BE SEARCHED are further described as follows:

a. Hewlett Packard M7000 desktop computer serial number MXK60804L3 and all hardware and software attached to, or otherwise accompanying this computer as seized;

b. Dell Dimension E521 desktop computer serial number HWC16C1 and all hardware and software attached to, or otherwise accompanying this computer as seized;

c. Hewlett Packard Touch Smart 1Q770 computer serial number CNH7010011 and all hardware and software attached to, or otherwise accompanying this computer as seized;

d. Sony Vaio laptop computer serial number VGNUX280P and all hardware and software attached to, or otherwise accompanying this computer as seized;

ATTACHMENT B

ITEMS TO BE SEIZED

1. The following are the ITEMS TO BE SEIZED from the ITEMS TO BE SEARCHED, which constitute evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 2251, production of child pornography as it relates to interstate or foreign commerce, Title 18, United States Code, Section 2252A(a)(5)(B), possession of child pornography, Title 18 United States Code, Section 2252A(a)(2)(A), distribution receipt or distribution of child pornography, and Title 18 United States Code, Section 2252A(a)(2)(B), receipt or distribution of material containing child pornography:

a. Files or records that tend to identify the person(s) in control, possession, and ownership of the computers identified in ATTACHMENT A or of any other computers, including, but not limited to, canceled mail, photographs, personal telephone books, diaries, bills and statements, identification cards and documents, airline tickets and related travel documents, bank books, checks, and check registers, public storage facilities receipts, computer registration records and sales receipts;

b. Images of child pornography, or materials containing child pornography as defined in 18 U.S.C. Section 2256, which visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography;

c. Files and records reflecting ownership, purchase, possession, or use of computer devices or peripherals such as web cameras and other video and audio recording devices, that could be used to transmit live images over the Internet or record images for later transmission over the Internet;

d. Files and records relating to the provision of internet service, including billing and toll records;

e. Correspondence that are indicia of production, possession, receipt, or distribution of child pornography including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, receipt, production, distribution, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

f. Correspondence relating or referring to exploitation of children including, but not limited to electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce of child pornography as defined in 18 U.S.C. § 2256, including by United States mail or by computer.

g. Files and records pertaining to possession, production, receipt or distribution of child pornography, as defined in 18 U.S.C. § 2256, including but not limited to:

(1) Envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat

logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

(2) Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

h. Any files or records relating to the exploitation of minors.

i. Any files or records identifying individual e-mail addresses and internet chat room names;

j. Any files or records showing the acquisition and/or sale of computer hardware, computer software, computer documentation, and/or computer passwords and other data security devices;

k. Any files or records evidencing occupancy or ownership of any residences and storage units registered to, owned by, or controlled by JAMES ALBERT SWEENEY II, including, but not limited to copies of utility and telephone bills, mail envelopes, addressed correspondence canceled mail, photographs, personal telephone books, diaries, bills and statements, identification cards and documents, airline tickets and related travel documents, bank books, checks, and check registers, and public storage facilities receipts.

l. Any files, records, programs, application or materials, including but not limited to, images and electronically stored computer data that would lead to the identity of any minors as depicted in electronic images or evidenced in electronic communications.

m. Mailing lists, mailing address labels and any and all documents and records pertaining to any correspondence between JAMES ALBERT SWEENEY II and any minor.

n. Any files or records related to ownership, control and use of digital cameras, camcorders, or other recording devices.

o. Electronic materials pertaining to the receipt of, or orders or requests for visual depictions of a minor involved in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

p. Names, lists of names or addresses and identifying information of minors (such as names and dates of birth of minors).

q. As used above, the terms files, records, programs, or correspondence includes files, records, programs, or correspondence created, modified or stored in any form including electronically.

ATTACHMENT C

0718070 1 062707 02

2007 JUN 27 AM 9:27

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

EXPERIENCE AND TRAINING OF AFFIANT

I, Aaron L. Ward, am an Investigator with the California Department of Justice (DOJ), Special Crimes Unit, Office of the Attorney General. I have been employed as an Investigator with the Department of Justice since April 2, 2001. Prior to my employment as an investigator with the California Department of Justice, I was an United States Postal Inspector assigned to the Southern California Division of the United States Postal Inspection Service. I retired from the position of Postal Inspector on March 30, 2001, and took my current position. I was a Postal Inspector for twenty years. For the last ten years of my Inspection Service career, my responsibilities included investigating crimes involving mail fraud and supervising the activities of five other Postal Inspectors. I have extensive experience investigating crimes involving financial transactions, investment fraud schemes (including Ponzi schemes), and money laundering.

I completed an eleven week training course for Postal Inspectors at the United States Postal Inspection Service (USPIS) Academy at Potomac, MD. I have attended both basic and complex fraud training courses at the USPIS Academy in Potomac, MD. Additionally, I have received money laundering and asset forfeiture training at the USPIS Academy in Potomac, MD. I have received bankruptcy fraud training at the United States Attorney's Office (USAO), Central District of California (CDC), Los Angeles, CA.

I have provided training on workers' compensation fraud investigations to other postal inspectors. I have testified as an expert witness for the USAO, CDC, Los Angeles, CA., related to telemarketing fraud investigations.

I have been a participant in the United States Attorney's Office, Southern California, Investment Fraud Task Force, formed to pool resources and experiences in the investigation of violations and abuses in the area of "boiler room" schemes. I have also been a member of the County of Orange Boiler room Apprehension (COBRA) Task Force, which was comprised of various federal and state agencies that investigated alleged telemarketing "boiler room" fraud.

During my career as a postal inspector, I have been the affiant on approximately 60 search warrant affidavits, requesting to search and seize electronic files contained in computer equipment.

06270702

bank accounts, brokerage accounts, and records from business and residential premises. In virtually every instance in which a search warrant was issued, I found evidence of the crime alleged. I am familiar with the United States Code and the California Penal Code relating to financial crimes, conspiracy, and the rules of evidence.

INTRODUCTION

This case was referred to the Department of Justice, Office of the Attorney General, in April 2007, after complaints by investors about the individuals and companies discussed below. The Department of Justice enforcement attorney, Kirk Wallace, referred the case for the reason that it was believed the below described individuals were operating an endless chain marketing scheme and had defrauded investors of approximately $5 Million in unregistered stock, in addition to selling memberships, in violation of the California Corporate Securities laws, as well as the California Penal Code.

MISREPRESENTATIONS/OMISSIONS

On June 20, 2007, I reviewed a Desist and Refrain order against James Albert Sweeney, II, Richard Hickey, Patrick Ryan, and Rick Deluca doing business as Big Co op, Inc. and EZ.2Win.Biz, Inc. The Desist and Refrain (D and R) order was issued because James Albert Sweeney, II, Richard Hickey, Patrick Ryan, and Rick Deluca doing business as Big Co op, Inc. and EZ2Win.Biz were offering unregistered and unlicensed securities to the public. The D and R order pointed out that James Albert Sweeney, II, Richard Hickey, Patrick Ryan, and Rick Deluca doing business as Big Co op, Inc. and EZ.2Win.Biz, Inc. failed to advise their investors of the following:

1. That the public offering of Big Co op, Inc. stock still had not occurred several years after prior purchasers had been told it would occur.
2. That Big Co op, Inc. had made no significant effort to prepare the required documents such as audited financial statements or business plans which would be required to take the company public and had not applied to any State or Federal regulatory agencies to be permitted to offer publicly traded stock.
3. That the statements made to license purchasers in 2006 that Thomas Wiesel Partners was going to take Big Co op, Inc. public in December of 2006 was also untrue in that

06270702

no request had been made at that time by Big Co op. Inc. to Thomas Wiesel Partners to take any action or make any preparations to take Big Co op, Inc. public in December of 2006, or at any other time.

4. That purchasers of licenses were not told that Big Co op, Inc. and EZ2Win.Biz had operated at a loss in each year of its existence and had a continuing loss of over 4 million dollars by the end of 2006.

5. That almost all of the income for the company was generated by the sale of licenses and fees charged to participants in the multilevel marketing scheme.

6. That income from Big Co op, Inc.'s "core business" of making commissions from the sale of goods and services from third parties through the Big Co op internet shopping network amounted to less than 1% of the company's income.

7. That the certified public accountant who prepared the financial statements for Big Co op, Inc. for the years 2003 2006 had included a notice with the statements for each of those years that Big Co op, Inc. had not been able to market its products at amounts sufficient to recover its service and administrative costs and had suffered consecutive losses for 5 years. The accountant's notice concluded "because of uncertainties surrounding the ability of the company to continue its operations and to satisfy its creditors on a timely basis, there is doubt about the company's ability to continue as a going concern."

INVESTIGATION AIROSA

On May 29, 2007, I interviewed Joy Paguiso Airosa who told me the following:

1. In response to an investment tip from a neighbor she and her mother contacted Patrick Ryan, President of EZ2Win.Biz. Ryan told them that Big Co op. Inc. was a great investment opportunity that would be going public soon. The stock would be worth $50.00 per share when the company goes public.

2. Ryan told her that Big Co op, Inc. was an Internet shopping business that had discount agreements with many big retail companies. like Sears. J.C. Penny. Nordstrom's, and Target stores.

06270702

3. Ryan and others compared Big Co op. Inc., with Google.

4. Based on this information her mother, on October 24, 2006, wrote a personal check (number 643) in the amount of $25,000.00 made payable to EZ2Win.Biz as an investment in Big Co op. Inc.

5. Her mother and she didn't like the way Big Co op, Inc. handled their paperwork. For instance, it took the company until December 18, 2006, to get their stock certificate (for 28,000 shares) to them. They requested their money back soon after they invested.

6. After many telephone calls and e mail messages, on December 20, 2006, they got their money back in the form of a check ($25,000) from another investor, not the company.

ALGREEN

On May 29, 2007, I interviewed Mrs. Ann Algreen who told me the following:

1. Her deceased husband made the investment in Big Co op, Inc. She attended some meetings with him and was involved in some conversations with Patrick Ryan who got him involved with the investment.

2. Her husband met Ryan at the country club where they all golfed. Ryan latched onto her husband who treated him like a son.

3. Ryan told them Big Co op was going public. As a result of Ryan's representations her husband invested $104,000.00 in Big Co op. Inc.

4. At some point her husband and she started to have doubts about Big Co op. Inc. Ryan kept putting them off when they asked him about the company going public.

5. Ryan kept giving her husband and her excuses for the company not going public. One excuse he gave was that the company was meeting with overseas investors. Ryan also talked about the company doing something in India.

6. When her husband knew he was dying, he asked Ryan for their money back. Ryan told him he would have to check with his father, James Sweeney.

///

06270702

7. Before he died, her husband had a meeting with James Sweeney at Sweeney's office in downtown Riverside. Their investment advisor accompanied her husband to this meeting. Sweeney refused to give her husband their money back.

CICHY

On June 6, 2007, I interviewed Mr. Ron Cichy who told me the following:

1. He met Patrick Ryan at a bar in downtown Riverside (just down the street from the business office). Ryan told him he had a great investment opportunity with his Internet shopping company.
2. He befriended Ryan and they joined the Canyon Crest Country Club together.
3. He made several investments with Big Co op, Inc. beginning in November 2001 when he invested $35,000.00 with the company. Ryan told him the stock was worth $1.00 per share, but would increase in value when the company goes public. He invested a total of $70,000.00 with the company.
4. In addition to investments in the company, he gave Ryan numerous personal loans totaling in excess of $50,000. He also paid many of Ryan's bills.
5. Ryan has since repaid most of the $50,000.00 of personal loans, with company checks [Ryan Enterprises (drawn on a Wells Fargo Bank account) and Big Co op, Inc. (drawn on an Inland Empire National Bank account)].
6. Ryan told him the company was making money and was in the black. In fact, Ryan told him that the company was making $1 million per month.
7. Ryan told him "the auditors" were ready to go into the company and do an audit so that the company would be closer to going public.
8. Ryan also mentioned a reverse merger being in the works in order to take the company public.
9. He found out that the company was engaged in the sale of illegal securities. Ryan told him 2 months ago (April 2007) that the company has spent $500,000.00 in legal fees to make the company legal.

///

06270702

10. Ryan gave him numerous reasons for the company not going public. One reason was that a group of Norwegians were going to invest millions of dollars in Big Co op, Inc.

11. The company would give away expensive gifts as inducements at sales meetings for the multi level marketing program ran by Big Co op, Inc.

DAKOTA

On June 15, 2007, I interviewed Mr. John Dakota who told me the following:

1. He invested $20,000.00 in Big Co op, Inc. after being told by Patrick Sweeney (a/k/a Patrick Ryan) that it was a great opportunity.

2. Big Co op, Inc. would be going public within 90 days from his investment date or he would get his money back.

3. After 90 days the company still had not gone public.

4. He asked Ryan why the company hadn't gone public and he was told it would be another 90 days.

5. When the second 90 days passed and the company hadn't gone public, he asked Ryan for his money back.

6. Ryan told him he would have to submit a letter to the company in order for the legal channels to take place.

7. When he didn't get a response to his first letter, he telephoned Ryan and told him he would go to the California Department of Corporations and to the News Media if he didn't get his money back.

8. Ryan told him he would get his money back, but it would take approximately 4 months at $5,000.00 per month to do so. He got his money back within 4 months.

9. As he recalls the checks paying back his investment were drawn on an account at Wells Fargo Bank.

10. When he invested with the company, Ryan was the President of EZ2Win.Biz, which is the marketing side of Big Co op, Inc. James Sweeney was the CEO of Big Co op, Inc.

WALLING

On June 20, 2007, I contacted Mr. Russell Walling, Owner/Building Manager, 3666 University Avenue, Suite 405, Riverside, California. He told me the following:

1. He has known James Sweeney doing business as Big Co op, Inc. for 8 or 9 years, when he moved into the building.
2. Sweeney and his adopted son, Patrick Ryan, seemed to alternate as president of the company.
3. He has tried to help Sweeney with his business over the years and consequently Sweeney owes him $229,000.00 in back rent over a 3 or 4 year period.
4. On or about June 6, 2007, Sweeney moved out of the building without paying his back rent.
5. Mr. Walling took possession of 9 Dell desktop computers belonging to Sweeney and his business; Sweeney and his business associates had abandoned the computers. After taking the nine (9) Dell desktop computers from the Big Co-op offices, Mr. Walling had the entrance doors to the 3rd floor re-keyed.
6. Sweeney took the computer that was in his office, Ryan took the computer that was in his office; and Ryan's ex wife, Kelli Ryan, who was also the company's chief financial officer/bookkeeper, took the computer that was in her office.
7. He has the 9 Dell computers on tables in a storage room in the basement of the building.
8. He knows that Sweeney and Ryan did their business banking at Wells Fargo Bank, which is down the street on University; and the Inland Empire National Bank, which is on the mall on Main Street.

OBSERVATIONS ON THE THIRD (3RD) FLOOR

On June 20, 2007, Mr. Walling gave me a tour of the third (3rd) floor of his building. This is the floor space that was occupied by Sweeney and his associates doing business as Big Co-op, Inc. and EZ2Win.Biz. While touring the third (3rd) floor of the building, I observed the following:

///

06270702

1. Walling unlocked the front entrance door to the suite of offices on the third (3rd) floor with a key that was on a large ring with other keys.

2. I observed a large open area that ran from one end of the third floor to the other end. This open area had individual offices off of it. I estimated that there are 8 to 10 individual offices within the office suite. Some offices are larger than others. Mr. Walling told me that Sweeney and Ryan had the larger offices.

3. Inside most of the individual offices, I saw trash receptacles filled with what appeared to be computer instruction manuals, Big Co-op/EZ2Win.Biz business instruction manuals and other documents.

4. I observed the offices to be virtually empty except for the trash receptacles and some office furniture.

BANK LOCATIONS TO BE SEARCHED

With regard to the Wells Fargo Bank accounts at 3750 University Avenue, Riverside, California and the accounts at Inland Empire National Bank at 3737 Main Street, Suite 104, Riverside, California, based on the below information and my experience, I believe there is probable cause to believe that there are Ryan Enterprises, Big Co op, Inc. and EZ2Win.Biz, Inc., as well as Sweeney and Ryan financial records, which are on the premises and are evidence of the crimes described below.

BASEMENT STOREROOM LOCATION

With respect to the nine (9) Dell desktop computers currently being stored in the basement storeroom at the Walling Building, 3666 University Avenue, Riverside. California, based on the below information and my experience I believe there is probable cause to believe that there are business and financial records related to Ryan Enterprises, Big Co op. Inc. and EZ2Win.Biz, Inc., which are on the premises and are evidence of the crimes described below.

THIRD FLOOR WALLING BUILDING LOCATION

With respect to the third floor of the Walling Building. 3666 University Avenue, Riverside, CA 92501. based on the above information and my experience, I believe there is probable cause to believe that there are computer instruction manuals and Big Co-op, Inc./EZ2Win.Biz business

06270702

manuals and other documents in trash receptacles in the individual offices within the suite of offices on the third (3rd) floor, which are on the premises and are evidence of the crimes described below.

PERSONAL RESIDENCES

With respect to the personal residences of Patrick Michael Ryan, 1048 Peter Christian Circle, Corona, California 92881; and the residence of Kelli Ann Ryan, the company's chief financial officer/bookkeeper, 29449 Tours Street, Lake Elsinore, California , based on the information described herein and my experience I believe there is probable cause to believe that there are Ryan Enterprises, Big Co op, Inc. and EZ2Win.Biz, Inc., business records and financial information, which are on the premises and is evidence of the crimes described below.

Based on the information contained herein, my experience and the experience of other agents and Investigators with whom I have worked, I believe there is probable cause to believe that the bank records and the electronic records requested in this affidavit and stored in the nine (9) Dell desktop computers kept in the basement storage room of the Walling Building and the two (2) computers kept in the separate, personal residences of Patrick Ryan and his ex-wife, Kelli Ann Ryan, as well as the instruction and business manuals contained in trash receptacles on the third (3rd) floor of the Walling Building contain evidence of the on going securities fraud and theft perpetrated on the public by James Albert Sweeney II and Patrick Michael Ryan doing business as Ryan Enterprises, Big Co op, Inc. and EZ2Win.Biz, Inc., as described below:

APPLICABLE CRIMINAL STATUTES

Section 25401 of the California Corporate Securities law states that it is unlawful for any person to offer or sell a security in this state or buy or offer to buy a security in this state by means of any written or oral communication which also includes an untrue statement of material fact or omits to state a material fact necessary in order to make the statements made in light of the circumstances under which they were made, not misleading.

Section 25110 of the California Corporation Securities Law states that it is unlawful for any person to offer or sell in this state any security in an issuer transaction unless such sale has been qualified under section 25111, 25112 or 25113 or unless such security or transaction is exempted or not subject to qualification.

06270702

Section 25540(a) of the California Corporate Securities Law states any person who willfully violates any provision of the Corporate securities Law of 1968, or who willfully violates any rule or order under said division, shall upon conviction be fined not more than one million dollars ($1,000,000), or imprisoned in the state prison, or in county jail for not more than one year, or be punished by both fine and imprisonment.

Section 25540(b) of the California Corporate Securities law sates any person who willfully violates section 25400, 25401 or 25402, or who willfully violates any rule or order under the Corporate Securities Law of 1968, adopted pursuant to those provisions, shall upon conviction be fined not more than ten million dollars ($10,000,000), or imprisoned in the state prison for two (2), three (3), or five (5) years, or be punished by both fine and imprisonment.

Section 327 of the California Penal Code states that it is unlawful for any person to contrive, prepare, set up, propose, or operate any endless chain an "endless chain" means any scheme for the disposal or distribution of property whereby a participant pays a valuable consideration for the chance to receive compensation for introducing one or more additional persons into the participation in the scheme or for the chance to receive compensation when a person introduced by the participant introduces a new participant. This crime is punishable by imprisonment in the county jail not exceeding one year or in the state prison for 16 months, two or three years.

Section 487 of the California Penal code states that Grand Theft is committed in any of the following cases: (a) when the money, labor or real or personal property taken is of a value exceeding four hundred dollars ($400).

WELLS FARGO AND INLAND EMPIRE NATIONAL BANKS

On June 20, 2007, I went to the Wells Fargo Bank, which is down the street from the Walling Building (3666 University Avenue) and observed that the address is 3750 University Avenue (the Riverside Main Office), Riverside, California 92501.

On June 20, 2007, I went to the Inland Empire National Bank, which is on the mall on Main Street as described by Mr. Walling and learned the following:

1. The address is 3737 Main Street, Suite 104, Riverside, California 92501.

///

062 70702

2. Alice Henderson is the Operations Manager at this bank. She told me that:

a. She knows the business name Big Co op, Inc.

b. Account number: 001515756 is maintained at her branch.

c. Legal documents should be served on the main office at 3727 Arlington Avenue, Riverside, CA 92706.

During the investigation I reviewed the checks given me by investors Airosa/Paguio and Cichy and learned the following:

1. The check Paguio used to pay Big Co op, Inc (EZ2Win.Biz) showed the following:

a. The check number is 643 and is dated 10/24/2006; it is made payable to EZ2Win.Biz in the amount of $25,000.00.

b. The back of the check shows that it was deposited to an account titled EZ2Win.BIZ; the number is 6655853429 (I have seen this same series of numbers on a Wells Fargo Bank check written to Mr. Cichy).

2. One of the checks given me by Mr. Cichy was drawn on a Well Fargo Bank account (number: 6655851878). It is check number 1077 and is dated 1/10/2006. The check is in the amount of $1,000.00. The memo section of the check reads: "loan pay back to him." The account name is Ryan Enterprises, 3666 University Ave. FL 3, Riverside, CA 92501 3346.

3. Another check given me by Mr. Cichy shows the following:

a. The check number is 3209 drawn on Inland Empire National Bank, Riveside, CA 92501. The check is dated 6/8/2004.

b. The account name is Big Co op, Inc., 3666 University Ave. 3RD Floor, Riverside. CA 92501.

c. The account number is 001515756.

PERSONAL RESIDENCE PATRICK RYAN (A/K/A PATRICK SWEENEY)

When interviewed June 20, 2007, Mr. Russell Walling reported that Patrick Ryan had taken his desktop computer from his office on June 6 8, 2007. During the investigation I learned that

06270702

Patrick Ryan lives at 1048 Peter Christian Circle, Corona, California 92881. On June 25, 2007, I went to the address 1048 Peter Christian Circle, Corona, California 92881 and observed the following:

1. A dark blue Mercedes Benz bearing California license plate number "5YGT009" was parked in the driveway. Another dark colored Mercedes Benz bearing no license plates was parked on the street in front of the house.

2. A subsequent check with the California Department of Motor Vehicles revealed that plate number "5YGT009" is registered to Patrick Ryan and/or Kelli Ryan, 1048 Peter Christian Circle, Corona, California.

PERSONAL RESIDENCE KELLI RYAN

When he was interviewed on June 20, 2007, Mr. Walling told me that Kelli Ryan was the chief financial officer/bookkeeper for the Big Co op, Inc. and EZ2Win.Biz business. He said he knows that she took the desktop computer that she used at the business. During the investigation, I learned that Kelli Ryan lives at 29449 Tours Street, Lake Elsinore, California. On June 25, 2007, I went to the address 29449 Tours Street, Lake Elsinore, California, and observed the following:

1. A new looking dark blue Mercedes Benz bearing personalized California license plates "SXYCFO" was parked in the driveway. There were two (2) other vehicles parked in the driveway also. One was a dark colored Cadillac Escalade with no plates; the other was a dark colored SUV bearing personalized California license plates "WUCARDZ."

2. A subsequent check with the California Department of Motor Vehicles revealed that plate number "5YGT009" is registered to Kelli Ann Ryan, 29449 Tours Street, Lake Elsinore, California.

SEIZURE OF DIGITAL EVIDENCE

With respect to the nine (9) Dell computers currently being stored in the basement storeroom of the Walling Building at 3666 University Avenue, Riverside, California 92501; and the three (3) desk top computers taken from the business location by James Albert Sweeney, Patrick Michael Ryan, and Patrick Ryan's ex wife, Kelli Ann Ryan and believed to be kept at their personal residences, I have consulted with Robert Werbick, whom I have known and worked with for over 15 years. Robert Werbick has been employed as a Postal Inspector with the United States Postal Inspection Service, Los Angeles Division since November 1991. Beginning in December 2001, Postal Inspector Werbick has been assigned to the Forensic Laboratory Services Division, Dulles, Virginia as Program Manager, Digital Evidence Unit domiciled in Anaheim, CA, where his duties have included the investigation of criminal offenses including high technology crime, account fraud, check fraud, and identity theft and the forensic examination of computers. Postal Inspector Werbick possesses a Bachelor of Science degree in electrical engineering from California Polytechnic University, Pomona, California. He has attended numerous specialized training courses in forensic science, including training in Encase forensic science.

Based on my training, experience and my conversations with Postal Inspector Werbick, I am aware of the following: (1) that individuals engaged in securities fraud and grand theft often use computers as tools of their crime, to store clients' personal and account information, to create company records, correspondence to clients/customers, and company update information and to store company and personal financial transaction records; (2) that suspects use computers to obtain goods, services, and/or other personal and company assets; (3) that computer users will commonly keep computers and computer systems in their homes and places of employment; (4) that computer users frequently back up copies of software to guard against loss if their computer malfunctions; they keep those backup copies at their residence and/or place of employment; and (5) that software and digital data is portable and is often transported to and from residences in automobiles and is occasionally hidden in automobiles.

In addition, Postal Inspector Werbick advised me why all computers and computer equipment must be removed from search warrant sites and searched under controlled circumstances. Because of the ways in which computer technologies store or process data, files relating to criminal investigations are often stored with unrelated records. In order to determine which records may be seized pursuant to a search warrant, it is necessary to use appropriate forensic software to open and

///

///

06270702

view the contents of all files. Postal Inspector Werbick further advised me that the file name in the folder/directory is not a reliable indicator of the true nature of its contents, especially where there may be a desire on the user's part to conceal certain records.

Postal Inspector Werbick has also been trained in methods to recover hidden, deleted, and erased files. Based on his experience and training, he advises me that digital files reside, in whole or in part, on a computer's hard drive or other external electronic storage media until they are overwritten. Under many operating systems software (including Microsoft Windows 95 or higher), it is frequently possible to reconstruct deleted or erased files, as well as the fact of the deletion and the time and date of the deletion. Such facts can be evidence of an attempt to destroy, hide or fabricate evidence, and may be evidence of consciousness of guilt. According to Postal Inspector Werbick, computer users may also conceal data through a number of methods, including the use of misleading filenames and extensions. For example, files with the extension ".jpg" are digital image files. However, a computer user could change a ".jpg" file extension to ".txt" or ".dll," in order to create an appearance that a digital image is actually a text or system file. It is often difficult for an investigator to notice such anomalies without conducting a properly controlled forensic examination at a location away from the search site.

Postal Inspector Werbick advised me that conducting a search of a computer system's files, documenting the search, and making evidentiary and discovery copies is a lengthy and time consuming process, particularly with the increased data storage capacity of newer computers. He said it is also necessary to determine that no security devices are in place, both hardware and software, which could cause the destruction of evidence during the search. He said in some cases it is impossible even to conduct the search without expert technical assistance, especially if the data is stored on a network server and/or Unix operating system. He said expert technical assistance may also be required if the computer system and files have been protected using an encryption method. Since computer evidence is extremely vulnerable to tampering or destruction through error, electrical outages, and other causes, the removal of the system from the premises will greatly assist in retrieving the records authorized to be seized, while avoiding destruction or deliberate alteration of the records. He said it would be very difficult to search the computer system's files on the

062 70702

premises during the execution of a search warrant. Instead, a search could take several weeks or months, depending on the technical difficulties encountered. He told me that in almost every instance the suspect's computer(s) and removable electronically stored media should be removed from the crime scene and their contents be examined in a controlled environment to preserve the evidentiary integrity of the data.

Postal Inspector Werbick advised me that any use of a subject's computer to examine files should be avoided, since it could be rigged to destroy or alter data. He also told me that it is impossible to ensure that any equipment brought by law enforcement personnel to a search site could be used to adequately examine storage media present at the location, since the type and quantity of storage media is usually not known prior to conducting a search. In addition, it is impossible to predict which application programs, drivers, and other software (out of hundreds available on the market) have been used by the subject to create files stored on the computer media.

For this reason, Postal Inspector Werbick advised me that all software associated with any seized computer must also be seized since it would be impossible, without examination, to determine if it is standard commercially available software. He said in many instances it is necessary to examine the software applications used to create files in order to read the files. Additionally, without examination, it is impossible to determine if a disk, purporting to contain a standard commercially available software program. Is also being used to store data or information relevant to the ongoing investigation.

I was also advised by Postal Inspector Werbick that system documentation, instruction manuals, and software manuals relating to the computer system also need to be seized in order to properly operate that specific system, and to accurately obtain and copy the records and files authorized to be seized. This documentation may also further assist in establishing the ownership and/or the operator of the computer system being seized. He also told me that computer users frequently employ passwords to protect their data files and records. He said that in many instances the computer user will often write passwords in their system manuals, notebooks, on post it notes, etc., and it is therefore necessary to seize all written material that is in close proximity of a computer system being seized.

06270702

premises during the execution of a search warrant. Instead, a search could take several weeks or months, depending on the technical difficulties encountered. He told me that in almost every instance the suspect's computer(s) and removable electronically stored media should be removed from the crime scene and their contents be examined in a controlled environment to preserve the evidentiary integrity of the data.

Postal Inspector Werbick advised me that any use of a subject's computer to examine files should be avoided, since it could be rigged to destroy or alter data. He also told me that it is impossible to ensure that any equipment brought by law enforcement personnel to a search site could be used to adequately examine storage media present at the location, since the type and quantity of storage media is usually not known prior to conducting a search. In addition, it is impossible to predict which application programs, drivers, and other software (out of hundreds available on the market) have been used by the subject to create files stored on the computer media.

For this reason, Postal Inspector Werbick advised me that all software associated with any seized computer must also be seized since it would be impossible, without examination, to determine if it is standard commercially available software. He said in many instances it is necessary to examine the software applications used to create files in order to read the files. Additionally, without examination, it is impossible to determine if a disk, purporting to contain a standard commercially available software program, is also being used to store data or information relevant to the ongoing investigation.

I was also advised by Postal Inspector Werbick that system documentation, instruction manuals, and software manuals relating to the computer system also need to be seized in order to properly operate that specific system, and to accurately obtain and copy the records and files authorized to be seized. This documentation may also further assist in establishing the ownership and/or the operator of the computer system being seized. He also told me that computer users frequently employ passwords to protect their data files and records. He said that in many instances the computer user will often write passwords in their system manuals, notebooks, on post it notes, etc., and it is therefore necessary to seize all written material that is in close proximity of a computer system being seized.

Therefore, I request that investigating officers be authorized, at their discretion, to seize all "computer systems," "computer program or software," and "supporting documentation" as defined by Penal Code section 502, subdivision (b), including any peripherals, and any supporting hardware, software, and to conduct an off site search of the seized items for the evidence described in this affidavit. I further request that investigating officers, and those agents acting under the direction of the investigating officers, be authorized to access all computer data to determine if the data contains "property," "records," and "information," and that, if necessary, investigating officers be authorized to employ the use of outside experts, acting under the direction of the investigating officers, to access and preserve computer data. I request authorization for investigating officers to seized any digital evidence found during the execution of this search warrant, to transported such evidence from the search location, and to conduct a search and analysis at a location designated by investigating officers. With respect to any above described computer found during a search executed within ten days of the issuance of this warrant, I request authorization for officers or their agents to seize, transport, and analyze such computers, and that such a search may continue beyond ten (10) days after the issuance of the search warrant.

I also request permission to videotape and/or photograph the execution of this search warrant. I expect to examine computer(s) at the scene of the search. Those computers may be operating when I arrive at the premises. The images on the screens of the computers are transient, meaning that they disappear when the computer is turned off. I need to be able to videotape and/or photograph any such images because they may be evidence (e.g., incriminating documents being written by the user when the search warrant is executed). The videotape or photographs may be useful in documenting what was done to the computers. Photography of the location and persons present at the scene is also often helpful in showing possession of the premises and evidence of association of the parties.

CONCLUSION

Based on the information contained herein, my experience and the experience of other agents and investigators with whom I have worked, I believe there is probable cause to support the issuance of search warrants as set forth in Penal Code Section 1524 to search for any accounts listed in Attachment "A" and to provide all information from those accounts to me. I believe there is

06270702

probable cause to support the issuance of a search warrant as set forth in Penal Code Section 1524 to search for and seize the nine (9) Dell computers currently being stored by Mr. Russell Walling in the basement of his office building as well as the desk top computers taken from the business location and believed to be kept at the personal residences of Patrick Michael Ryan and Patrick Ryan's ex wife, Kelli Ann Ryan. Additionally, I believe there is probable cause to support the issuance of a search warrant as set forth in Penal Code Section 1524 to search for and seize financial and business records as well as computer and business manuals currently kept in trash receptacles in offices on the third (3rd) floor of the Walling Building. These documents and records will assist in determining if James Albert Sweeney II and Patrick Michael Ryan doing business as Ryan Enterprises, Big Co op, Inc. and EZ2Win.Biz, Inc., have committed grand theft and fraud.

Deputy Attorney General Patricia Fusco has reviewed this document.

Given under my hand and dated this 27 day of June 2007.

Aaron L. Ward 7/19/2007

Subscribed and sworn to before me this 27 day of June 2007, at 9:30 A.M. P.M.

JUDGE OF THE SUPERIOR COURT

CLERK

BY

DEPUTY CLERK

ATTACHMENT D

0718070

RECEIVED
SUPERIOR COURT OF CALIF.
COUNTY OF RIVERSIDE
2007 JUL 18 AM 9:41
BY

Supplemental

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

EXPERIENCE AND TRAINING OF AFFIANT

I, Aaron L. Ward, am an Investigator with the California Department of Justice (DOJ), Special Crimes Unit, Office of the Attorney General. I have been employed as an Investigator with the Department of Justice since April 2, 2001. Prior to my employment as an investigator with the California Department of Justice, I was a United States Postal Inspector assigned to the Southern California Division of the United States Postal Inspection Service. I retired from the position of Postal Inspector on March 30, 2001, and took my current position. I was a Postal Inspector for twenty years. For the last ten years of my Inspection Service career, my responsibilities included investigating crimes involving mail fraud and supervising the activities of five other Postal Inspectors. I have extensive experience investigating crimes involving financial transactions, investment fraud schemes (including Ponzi schemes), and money laundering.

I completed an eleven-week training course for Postal Inspectors at the United States Postal Inspection Service (USPIS) Academy at Potomac, MD. I have attended both basic and complex fraud training courses at the USPIS Academy in Potomac, MD. Additionally, I have received money laundering and asset forfeiture training at the USPIS Academy in Potomac, MD. I have received bankruptcy fraud training at the United States Attorney's Office (USAO), Central District of California (CDC), Los Angeles, CA.

I have provided training on workers' compensation fraud investigations to other postal inspectors. I have testified as an expert witness for the USAO, CDC, Los Angeles, CA., related to telemarketing fraud investigations.

I have been a participant in the United States Attorney's Office, Southern California, Investment Fraud Task Force, formed to pool resources and experiences in the investigation of violations and abuses in the area of "boiler-room" schemes. I have also been a member of the County of Orange Boiler-room Apprehension (COBRA) Task Force, which was comprised of various federal and state agencies that investigated alleged telemarketing "boiler-room" fraud.

///

///

ATTACHMENT D

07180070

RECEIVED SUPERIOR COURT OF CALIF. COUNTY OF RIVERSIDE 2007 JUL 18 AM 9:41 BY. Supplemental

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

EXPERIENCE AND TRAINING OF AFFIANT

I, Aaron L. Ward, am an Investigator with the California Department of Justice (DOJ), Special Crimes Unit, Office of the Attorney General. I have been employed as an Investigator with the Department of Justice since April 2, 2001. Prior to my employment as an investigator with the California Department of Justice, I was a United States Postal Inspector assigned to the Southern California Division of the United States Postal Inspection Service. I retired from the position of Postal Inspector on March 30, 2001, and took my current position. I was a Postal Inspector for twenty years. For the last ten years of my Inspection Service career, my responsibilities included investigating crimes involving mail fraud and supervising the activities of five other Postal Inspectors. I have extensive experience investigating crimes involving financial transactions, investment fraud schemes (including Ponzi schemes), and money laundering.

I completed an eleven-week training course for Postal Inspectors at the United States Postal Inspection Service (USPIS) Academy at Potomac, MD. I have attended both basic and complex fraud training courses at the USPIS Academy in Potomac, MD. Additionally, I have received money laundering and asset forfeiture training at the USPIS Academy in Potomac, MD. I have received bankruptcy fraud training at the United States Attorney's Office (USAO), Central District of California (CDC), Los Angeles, CA.

I have provided training on workers' compensation fraud investigations to other postal inspectors. I have testified as an expert witness for the USAO, CDC, Los Angeles, CA., related to telemarketing fraud investigations.

I have been a participant in the United States Attorney's Office, Southern California, Investment Fraud Task Force, formed to pool resources and experiences in the investigation of violations and abuses in the area of "boiler-room" schemes. I have also been a member of the County of Orange Boiler-room Apprehension (COBRA) Task Force, which was comprised of various federal and state agencies that investigated alleged telemarketing "boiler-room" fraud.

///

///

During my career as a postal inspector, I have been the affiant on approximately 60 search warrant affidavits, requesting to search and seize electronic files contained in computer equipment, bank accounts, brokerage accounts, and records from business and residential premises. In virtually every instance in which a search warrant was issued, I found evidence of the crime alleged. I am familiar with the United States Code and the California Penal Code relating to financial crimes, conspiracy, and the rules of evidence.

INTRODUCTION

This case was referred to the Department of Justice, Office of the Attorney General, in April 2007, after complaints by investors about the individuals and companies discussed below. The Department of Corporations (DOC) enforcement attorney, Kirk Wallace, referred the case for the reason that it was believed the below-described individuals were operating an endless-chain marketing scheme and had defrauded investors of approximately $5 Million in unregistered stock. In addition to selling memberships, in violation of the California Corporate Securities laws, as well as the California Penal Code. The DOC has issued two Desist and Refrain Orders against James Albert Sweeney, Big Co-Op, Inc. and EZ2Win.Biz and others. After the most recent Desist and Refrain Order was served, Attorney Wallace informed us that Mr. Sweeney had started a new company to continue Big Co-Op's Business. The name of that business is Together4Good, a Nevada Corporation.

This supplemental affidavit is being submitted in support of applications for search warrants on the residence of James Albert Sweeney, CEO, Big Co-op, Inc. and EZ2Win.Biz, 4555 Mission Inn Avenue, Riverside, California and two (2) storage units maintained by Sweeney at A-American Self-Storage at 2431 Rubidoux Avenue, Riverside, California

On Wednesday, June 27, 2007, Superior Court Judge J. A. Edwards authorized six search warrants (No: 06270702) relating to this matter. The Affidavit submitted in support of those six (6) search warrants is incorporated herein by reference and is attached to this supplemental affidavit as exhibit 1. One of the six search warrants was for the residence of Kelli Ann Ryan, CFO, Big Co-op, Inc. and EZ2Win.biz. I was a member of the task force that searched Ms. Ryan's residence. During the search of Ms. Ryan's residence, she told me the following:

0718070 1

a. She resigned her position at Big Co-op, Inc and EZ2Win.Biz in May 2007.

b. In early June 2007, James Sweeney moved his business out of the offices at 3666 University Avenue, 3rd Floor, Riverside, CA.

c. Sweeney took desktop computer that she used to use in her work for Big Co-Op, Inc/EZ2Win.Biz, wiped the computer's hard drive, and then gave the computer to her.

d. The computer Sweeney gave to her still has the company's (Big Co-Op, Inc/EZ2Win.Biz) financial files on it in the form of QuickBooks files.

e. She has spoken to Richard Hickey who used to work with her at Big Co-Op, Inc/EZ2Win.Biz and he told her he packed up a number of boxes with business records and took them to Sweeney's personal residence and placed many of the boxes in Sweeney's garage. When the garage got too full he took some boxes to the storage units.

f. Sweeney lives at 4555 Mission Inn Avenue, Riverside, California.

g. Sweeney had 3 storage units at A-American Self-Storage. Riverside, California. She believes he now has two (2) units there.

On Monday, July 2, 2007, I went to the address 4555 Mission Inn Avenue, Riverside, California, and observed the following:

h. The residence is a 2-story single-family residence on the north side of Mission Inn Avenue. Redwood Drive is to the east. It is dark tan in color and trimmed in a maroon and blue. The residence has an orange colored, ceramic tile roof.

i. There is a balcony on the second floor of the residence.

j. Entrance to the residence is through a single glass door framed in wood (colored maroon). The entrance door is in the center of the residence.

k. There are 2 sets of stairs leading from the street to the entrance doors. There are 2 statutes of lions (white in color) on either side of the steps closest to the entrance door.

///

On Monday, July 2, 2007, I spoke with Postal Inspector Dave Zemke who told me that he had checked on the address, 4555 Mission Inn Avenue, with the Riverside Post Office and learned that James A. Sweeney receives mail at the address.

On Thursday, July 12, 2007, I went to the A-American Self-Storage at 2431 Rubidoux Avenue, Riverside, California and learned the following:

a. The above location is a commercial structure located in the city and the county of Riverside. It is has a gray exterior, trimmed in dark blue.

b. The property is clearly marked by signage at the intersection of Rubidoux and 24th Streets that reads: A-American Self Storage. The signage is on a white back ground with blue letters and three wavy horizontal lines (denoting the American Flag) after the first "A." The signage can be seen from Rubidoux Avenue and there is a sign on 24th Street.

c. Entrance to the self-storage unit is off of 24th Street. Unit numbers 142 and 162 are on the east side of the main driveway leading from 24th Street.

d. Unit number 142 is 10' by 18'. It is clearly marked by the numbers 142 that are white in color and are affixed to the wall on the storage unit about ½ up the overhead door. There are red fire extinguishers mounted on the exterior of the storage units walls. The fire extinguishers are at every five storage units. Unit 142 is two (2) fire extinguishers from the entrance gate. The overhead door is dark blue in color.

e. Self-Storage unit 162 is 10' by 15'. It is located on the same side of

07180701

the driveway as unit 142. It is clearly marked by the numbers 162 that are white in color and are affixed to the wall on the storage unit about ½ up the overhead door. The overhead door is dark blue in color. Unit 162 is near the fifth fire extinguisher.

f. James Sweeney doing business as Big Co-op, Inc. rents units 142 and 162.

g. Sweeney was in earlier that day to argue about being assessed a late fee

of $20.00 for being late paying for the rental of the storage units.

APPLICABLE CRIMINAL STATUTES

Section 25401 of the California Corporate Securities law states that it is unlawful for any person to offer or sell a security in this state or buy or offer to buy a security in this state by means of any written or oral communication which also includes an untrue statement of material fact or omits to state a material fact necessary in order to make the statements made in light of the circumstances under which they were made, not misleading.

Section 25110 of the California Corporation Securities Law states that it is unlawful for any person to offer or sell in this state any security in an issuer transaction...unless such sale has been qualified under section 25111, 25112 or 25113...or unless such security or transaction is exempted or not subject to qualification...

Section 25540(a) of the California Corporate Securities Law states any person who willfully violates any provision of the Corporate securities Law of 1968, or who willfully violates any rule or order under said division, shall upon conviction be fined not more than one million dollars ($1,000,000). or imprisoned in the state prison, or in county jail for not more than one year, or be punished by both fine and imprisonment.

Section 25540(b) of the California Corporate Securities law sates any person who willfully violates section 25400, 25401 or 25402, or who willfully violates any rule or order under the Corporate Securities Law of 1968, adopted pursuant to those provisions, shall upon conviction be

0718070 1

fined not more than ten million dollars ($10,000,000), or imprisoned in the state prison for two (2), three (3), or five (5) years, or be punished by both fine and imprisonment. Section 327 of the California Penal Code states that it is unlawful for any person to contrive, prepare, set up, propose, or operate any endless chain...an "endless chain" means any scheme for the disposal or distribution of property whereby a participant pays a valuable consideration for the chance to receive compensation for introducing one or more additional persons into the participation in the scheme or for the chance to receive compensation when a person introduced by the participant introduces a new participant. This crime is punishable by imprisonment in the county jail not exceeding one year or in the state prison for 16 months, two or three years.

Section 487 of the California Penal code states that Grand Theft is committed in any of the following cases: (a) when the money, labor or real or personal property taken is of a value exceeding four hundred dollars ($400)...

CONCLUSION

With respect to the personal residence of James A. Sweeney I believe there is probable cause to support the issuance of a search warrant to search the premises described in Attachment A, location 1, as set forth in Penal Code Section 1524 to search for and seize financial and business records in any form as described in Attachment B. Records in the form of electronic files stored on computers will be treated as indicated in exhibit 1, pages 12 through 17. These documents and records will assist in determining if James Albert Sweeney II and Patrick Michael Ryan doing business as Ryan Enterprises, Big Co-op, Inc. and EZ2Win.Biz, Inc., have committed grand theft and fraud.

With respect to the 2 storage units maintained by James A. Sweeney at A-American Self-Storage, 2431 Rubidoux Avenue, Riverside, California, I believe there is probable cause to support the issuance of search warrants as set forth in Penal Code Section 1524 to search the self-storage units described in Attachment A, location 2 for and seize financial and business records in any form described in Attachment B. Records in the form of electronic files stored on computers will be treated as indicated in exhibit 1, pages 12 through 17. These documents and records will assist in

///

///

07180701

determining if James Albert Sweeney II and Patrick Michael Ryan doing business as Ryan Enterprises, Big Co-op, Inc. and EZ2Win.Biz, Inc., have committed grand theft and fraud.

Deputy Attorney General Patricia Fusco has reviewed this document.

Given under my hand and dated this ________ day of July 2007.

[signature]
Aaron L. Ward

Subscribed and sworn to before
me this 15th day of July 2007,
at ____ A.M./ P.M.

[signature]
JUDGE OF THE SUPERIOR COURT